



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for the Voice Print Activ! Voice Call Logger with Avaya Communication Manager and Avaya Application Enablement Services - Issue 1.0**

### **Abstract**

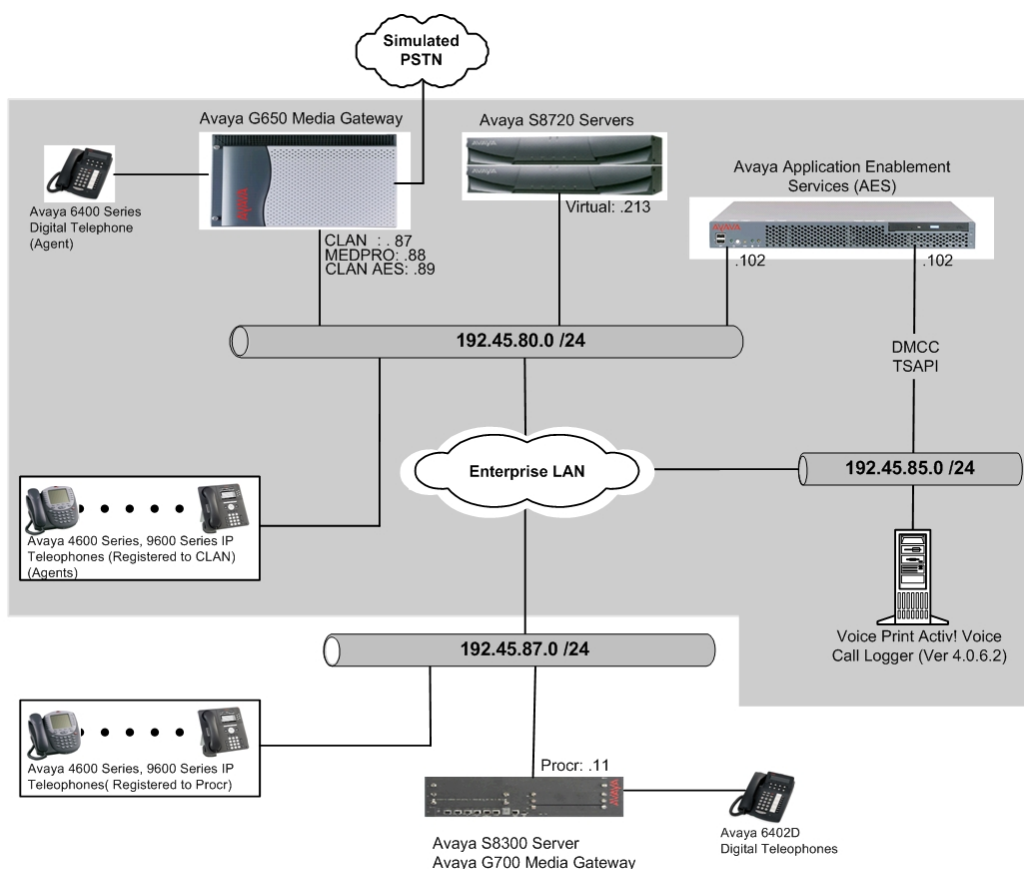
These Application Notes describe the procedures for configuring the Voice Print Activ! Voice Call Logger to monitor and record calls placed to and from stations, and to Vector Directory Numbers (VDN) on Avaya Communication Manager. When the recording of a call is desired, the Voice Print Activ! Voice Call Logger issues a Single Step Conference request through events acquired from the Telephony Services Application Programming Interface (TSAPI). In the configuration discussed in these Application Notes, Voice Print Activ! Voice Call Logger employs Device, Media and Call Control Application Programming Interface (API) virtual stations as recording ports. During compliance testing, Voice Print Activ! Voice Call Logger successfully recorded calls placed to and from stations, as well as calls placed to a VDN and then queued to an agent hunt/skill group.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describe a compliance-tested configuration comprised of an Avaya Communication Manager, an Avaya Application Enablement Services (AES) Server and the Voice Print Activ! Voice Call Logger. Activ! Voice Call Logger monitors, records, stores, and plays back phone calls for verification. Activ! Voice Call Logger uses TSAPI with an Avaya AES server to monitor stations, and/or VDNs, i.e. to obtain recording triggers and call information. Activ! Voice also uses the Device, Media and Call Control (DMCC) API with the Avaya AES server to register DMCC softphones that Activ! Voice Call Logger uses as recording ports. When recording of a call is desired, Activ! Voice Call Logger issues a Single Step Conference request through events acquired from TSAPI.

**Figure 1** provides the test configuration used for the compliance test. Note that actual configurations may vary. The solution described herein is also extensible to other Avaya Servers and Media Gateways. An Avaya S8300 Server with an Avaya G700 Media Gateway was included during the test, to provide a T1/ISDN-PRI trunk between two Avaya Communication Manager systems.



**Figure 1: Sample Test Configuration for the Voice Print Activ! Voice Call Logger Solution**

## 2. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration provided:

Equipment		Software/Firmware
Avaya S8720 Server		Avaya Communication Manager 5.0 (R015x.00.0.825.4)
Avaya G650 Media Gateway		-
	TN2312BP IP Server Interface	HW11 FW030
	TN799DP C-LAN Interface	HW20 FW017
	TN2302AP IP Media Processor	HW01 FW108
Avaya S8300 Server with Avaya G700 Media Gateway		Avaya Communication Manager 5.0 (R015x.00.0.825.4)
Avaya Application Enablement Services Server		R4.1.31.2
Avaya 4600 Series IP Telephones		
	4620SW (H.323)	2.8
	4625SW (H.323)	2.8
Avaya 9600 Series IP Telephones		
	9630 (H.323)	1.5
	9650 (H.323)	1.5
Avaya 6408D+ Digital Telephone		-
Analog Telephones		-
Voice Print Activ! Voice Server on Windows Microsoft 2003 Enterprise with Service Pack 2		4.0.6.2

## 3. Configure Avaya Communication Manager

This section provides the procedures for configuring a Computer Telephony Integration (CTI) link, Universal Caller ID (UCID), hunt/skill groups, vectors, Vector Directory Numbers (VDN), agents, agent login/logoff codes, and recording ports on Avaya Communication Manager. All the configuration changes in Avaya Communication Manager are performed through the System Access Terminal (SAT) interface. The highlights in the following screens indicate the values used during the compliance test.

### 3.1. AES Link between Avaya Communication Manager and Avaya Application Enablement Services Server

The Avaya AES server forwards CTI requests, responses, and events between the Voice Print Activ! Voice Call Logger and Avaya Communication Manager. The AES server communicates with Avaya Communication Manager over an AES link. Within the AES link, CTI links may be configured to provide CTI services to CTI applications such as the Voice Print Activ! Voice Call Logger. The following steps demonstrate the configuration of the Avaya Communication Manager side of the AES and CTI links. See **Section 4** for the details of configuring the AES side of the AES and CTI links.

Enter the **add cti-link m** command, where **m** is a number between 1 and 64, inclusive. Enter a valid Extension under the provisioned dial plan in Avaya Communication Manager, set the Type field to **ADJ-IP**, and assign a descriptive Name to the CTI link.

add cti-link 4		Page 1 of 2
CTI LINK		
CTI Link: 4		
Extension: 20006		
Type: ADJ-IP		
COR: 1		
Name: TSAPI		

Enter the **change node-names ip** command. In the compliance-tested configuration, the CLAN IP address was utilized for registering H.323 endpoint (Avaya IP Telephones and IP Softphones, and AES Device, Media and Call Control API stations) and the CLAN-AES IP address was used for connectivity to Avaya AES.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
CLAN	192.45.80.87	
CLAN-AES	192.45.80.89	
MEDPRO	192.45.80.88	
MEDPRO2	192.45.80.161	
S8300G700	192.45.87.11	
default	0.0.0.0	
procr	192.45.80.214	

Enter the **change ip-services** command. On **Page 1**, configure the Service Type field to **AESVCS** and the Enabled field to **y**. The Local Node field should be pointed to the **CLAN-AES** board that was configured previously in the IP NODE NAMES form in this section. During the compliance test, the default port was utilized for the Local Port field.

change ip-services						Page 1 of 4
IP SERVICES						
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	
AESVCS	y	CLAN-AES	8765			

On **Page 4**, enter the hostname of the AES server for the AE Services Server field. The server name may be obtained by logging in to the AES server using ssh, and running the command **uname -a**. Enter an alphanumeric password for the Password field. Set the Enabled field to **y**. The same password will be configured on the AES server in **Section 4.1**.

change ip-services					Page 4 of 4
AE Services Administration					
Server ID	AE Services Server	Password	Enabled	Status	
1:	server1	xxxxxxxxxxxxxxxxxx	y	idle	
2:					
3:					

## 3.2. Universal Call ID (UCID) Configuration

Enter the **display system-parameters customer-options** command. On **Page 3**, verify the Computer Telephony Adjunct Links field is set to **y**, to enable the UCID feature. If not, contact an authorized Avaya account representative to obtain the license.

```
change system-parameters customer-options                               Page 3 of 11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? n
    Access Security Gateway (ASG)? n              Authorization Codes? y
    Analog Trunk Incoming Call ID? n               CAS Branch? n
    A/D Grp/Sys List Dialing Start at 01? n       CAS Main? n
    Answer Supervision by Call Classifier? n        Change COR by FAC? n
    ARS? y                                          Computer Telephony Adjunct Links? y
    ARS/AAR Partitioning? y                       Cvg Of Calls Redirected Off-net? n
    ARS/AAR Dialing without FAC? y                DCS (Basic)? n
    ASAI Link Core Capabilities? n                DCS Call Coverage? n
    ASAI Link Plus Capabilities? n                DCS with Rerouting? n
    Async. Transfer Mode (ATM) PNC? n
    Async. Transfer Mode (ATM) Trunking? n        Digital Loss Plan Modification? n
    ATM WAN Spare Processor? n                    DS1 MSP? y
    ATMS? n                                        DS1 Echo Cancellation? n
    Attendant Vectoring? N
```

Enter the **change system-parameters features** command to enable the Universal Call ID (UCID) feature. On **Page 5** of the system-parameters features form, verify that the Create Universal Call ID (UCID) field is set to **y**, and the UCID Network Node ID field is specified. The UCID Network Node ID can be obtained by executing the **display dialplan parameters** command.

```
change system-parameters features                                     Page 5 of 17
                                FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
    Endpoint:                                     Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
    Switch Name:

    Emergency Extension Forwarding (min): 10
    Enable Inter-Gateway Alternate Routing? n

MALICIOUS CALL TRACE PARAMETERS
    Apply MCT Warning Tone? n    MCT Voice Recorder Trunk Group:

SEND ALL CALLS OPTIONS
    Send All Calls Applies to: station    Auto Inspect on Send All Calls? n

UNIVERSAL CALL ID
    Create Universal Call ID (UCID)? y    UCID Network Node ID: 1
```

On **Page 12** of the system-parameters features form, verify that the Send UCID to ASAI field is set to **y**.

change system-parameters features		Page 12 of 17
FEATURE-RELATED SYSTEM PARAMETERS		
AGENT AND CALL SELECTION		
MIA Across Splits or Skills? n		
ACW Agents Considered Idle? y		
Call Selection Measurement: current-wait-time		
Service Level Supervisor Call Selection Override? n		
Auto Reserve Agents: none		
ASAI		
Copy ASAI UII During Conference/Transfer? n		
Call Classification After Answer Supervision? n		
Send UCID to ASAI? y		
CALL MANAGEMENT SYSTEM		
Reporting Adjunct Release:		
BCMS/VuStats LoginIDs? y		
BCMS/VuStats Measurement Interval: hour		
BCMS/VuStats Abandon Call Timer (seconds):		
Validate BCMS/VuStats Login IDs? y		
Clear VuStats Shift Data: on-login		
Remove Inactive BCMS/VuStats Agents? N		

### 3.3. Hunt/Skill Groups, Agent Logins, and Call Vectoring

Enter the **display system-parameters customer-options** command. On **Page 6**, verify that the ACD, Expert Agent Selection (EAS) and Vectoring (Basic) fields are set to **y**. If not, contact an authorized Avaya account representative to obtain these licenses.

display system-parameters customer-options		Page 6 of 11
CALL CENTER OPTIONAL FEATURES		
Call Center Release: 3.0		
ACD? y		
Reason Codes? n		
BCMS (Basic)? y		
Service Level Maximizer? n		
BCMS/VuStats Service Level? n		
Service Observing (Basic)? y		
BSR Local Treatment for IP & ISDN? n		
Service Observing (Remote/By FAC)? y		
Business Advocate? n		
Service Observing (VDNs)? n		
Call Work Codes? n		
Timed ACW? N		
DTMF Feedback Signals For VRU? n		
Vectoring (Basic)? y		
Dynamic Advocate? n		
Vectoring (Prompting)? n		
Expert Agent Selection (EAS)? y		
Vectoring (G3V4 Enhanced)? n		
EAS-PHD? n		
Vectoring (3.0 Enhanced)? n		
Forced ACD Calls? n		
Vectoring (ANI/II-Digits Routing)? n		
Least Occupied Agent? n		
Vectoring (G3V4 Advanced Routing)? n		
Lookahead Interflow (LAI)? n		
Vectoring (CINFO)? n		
Multiple Call Handling (On Request)? n		
Vectoring (Best Service Routing)? n		
Multiple Call Handling (Forced)? n		
Vectoring (Holidays)? n		
PASTE (Display PBX Data on Phone)? n		
Vectoring (Variables)? n		
(NOTE: You must logoff & login to effect the permission changes.)		

Once the Expert Agent Selection (EAS) field is set to **y**, from the previous step, enter the **change system-parameters features** command. On **Page 11**, verify that the Expert Agent Selection (EAS) Enabled field is set to **y**. To enable the EAS feature, the Expert Agent Selection field in both the system-parameters customer-options form and the system-parameters features form should be set to **y**.

<b>change system-parameters features</b>	Page 11 of 18
FEATURE-RELATED SYSTEM PARAMETERS	
CALL CENTER SYSTEM PARAMETERS	
EAS	
Expert Agent Selection (EAS) Enabled? <b>y</b>	
Minimum Agent-LoginID Password Length:	
Direct Agent Announcement Extension:	Delay:
Message Waiting Lamp Indicates Status For: station	
VECTORIZING	
Converse First Data Delay: 0	Second Data Delay: 2
Converse Signaling Tone (msec): 100	Pause (msec): 30
Prompting Timeout (secs): 10	
Reverse Star/Pound Digit For Collect Step? n	
Store VDN Name in Station's Local Call Log? y	
SERVICE OBSERVING	
Service Observing: Warning Tone? y	or Conference Tone? n
Service Observing Allowed with Exclusion? n	
Allow Two Observers in Same Call? y	

Enter the **add hunt-group n** command, where **n** is an unused hunt group number. On **Page 1** of the hunt group form, assign a descriptive Group Name and Group Extension valid in the provisioned dial plan. Set the ACD, Queue, and Vector fields to **y**. When ACD is enabled, hunt group members serve as ACD agents and must log in to receive ACD split/skill calls. When Queue is enabled, calls to the hunt group will be served by a queue. When Vector is enabled, the hunt group will be vector controlled.

<b>add hunt-group 1</b>	Page 1 of 3
HUNT GROUP	
Group Number: 1	ACD? <b>y</b>
Group Name: test	Queue? <b>y</b>
Group Extension: 50011	Vector? <b>y</b>
Group Type: ucd-mia	
TN: 1	
COR: 1	MM Early Answer? n
Security Code:	Local Agent Preference? n
ISDN/SIP Caller Display:	
Queue Limit: unlimited	
Calls Warning Threshold:	Port:
Time Warning Threshold:	Port:

On **Page 2**, set the Skill field to **y**, which means that agent membership in the hunt group is based on skills, rather than pre-programmed assignment to the hunt group.

<b>add hunt-group 1</b>	Page 2 of 3
HUNT GROUP	
Skill? y	
AAS? n	
Measured: internal	
Supervisor Extension:	
Controlling Adjunct: none	
VuStats Objective:	
Redirect on No Answer (rings):	
Redirect to VDN:	
Forced Entry of Stroke Counts or Call Work Codes? n	

Enter the **add agent-loginID p** command, where **p** is a valid extension in the provisioned dial plan. On **Page 1** of the agent-loginID form, enter a descriptive Name and Password.

<b>add agent-loginID 50021</b>	Page 1 of 2
AGENT LOGINID	
Login ID: 50021	AAS? n
Name: Agent-1	AUDIX? n
TN: 1	LWC Reception: spe
COR: 1	LWC Log External Calls? n
Coverage Path:	AUDIX Name for Messaging:
Security Code:	LoginID for ISDN/SIP Display? n
	Password:
	Password (enter again):
	Auto Answer: station
	MIA Across Skills: system
	ACW Agent Considered Idle: system
	Aux Work Reason Code Type: system
	Logout Reason Code Type: system
	Maximum time agent in ACW before logout (sec): system
	Forced Agent Logout Time: :
WARNING: Agent must log in again before changes take effect	

On **Page 2**, set the Skill Number (SN) to the hunt group number previously created. The Skill Level (SL) may be set according to customer requirements.



Repeat this step as necessary to configure additional agent extensions.

```
add agent-loginID 50021                                     Page 2 of 2

                                AGENT LOGINID

    Direct Agent Skill:
Call Handling Preference: skill-level                        Local Call Preference? n

    SN      SL      SN      SL      SN      SL      SN      SL
1: 1       1       16:      31:      46:
2:         17:      32:      47:
3:         18:      33:      48:
```

Enter the **change vector q** command, where **q** is an unused vector number. Enter a descriptive Name, and program the vector to deliver calls to the hunt/skill group number. Agents that are logged into the hunt/skill group will be able to answer calls queued to the hunt/skill group.

```
change vector 1                                             Page 1 of 3

                                CALL VECTOR

    Number: 1                               Name: Queue to skill1

    Basic? y   EAS? y   G3V4 Enhanced? n   Meet-me Conf? n   Lock? n
    Prompting? n   LAI? n   G3V4 Adv Route? n   ANI/II-Digits? n   ASAI Routing? y
    Variables? n   3.0 Enhanced? n   CINFO? n   BSR? n   Holidays? n

01 wait-time 2 secs hearing ringback
02 queue-to skill 1 pri m
03
```

Enter the **add vdn r** command, where **r** is an extension valid in the provisioned dial plan. Specify a descriptive Name for the VDN and the **Vector Number** configured in the previous step. In the example below, incoming calls to the extension 50000 will be routed to testVDN50000, which in turn will invoke the actions specified in vector 1.

```
add vdn 50000                                             Page 1 of 2

                                VECTOR DIRECTORY NUMBER

    Extension: 50000
    Name*: testVDN50000
    Vector Number: 1

    Meet-me Conferencing? n
    Allow VDN Override? n
    COR: 1
    TN*: 1
    Measured: none

    1st Skill*:
    2nd Skill*:
    3rd Skill*:
```

Enter the **change feature-access-codes** command. Define the Auto-In Access Code, Login Access Code, Logout Access Code, and Aux Work Access Code.

```

change feature-access-codes                                     Page 5 of 6
                                FEATURE ACCESS CODE (FAC)

                                Automatic Call Distribution Features

                                After Call Work Access Code: 120
                                Assist Access Code: 121
                                Auto-In Access Code: 122
                                Aux Work Access Code: 123
                                Login Access Code: 124
                                Logout Access Code: 125
                                Manual-in Access Code: 126
                                Service Observing Listen Only Access Code: 127
                                Service Observing Listen/Talk Access Code: 128
                                Add Agent Skill Access Code: 130
                                Remove Agent Skill Access Code: 131
                                Remote Logout of Agent Access Code: 132

```

Enter the **add abbreviated-dialing group g** command, where **g** is the number of an available abbreviated dialing group. In the DIAL CODE list, enter the Feature Access Codes, created previously, for ACD Login and Logout.

```

add abbreviated-dialing group 1                               Page 1 of 1
                                ABBREVIATED DIALING LIST

                                Group List: 1                Group Name: Call Center
                                Size (multiple of 5): 5      Program Ext:                Privileged? n
DIAL CODE
11: 124
12: 125
13:

```

### 3.4. Recording Ports

The recording ports in this configuration are DMCC stations that essentially appear as IP Softphones, to Avaya Communication Manager. Each DMCC station requires an IP\_API\_A license. Note that this is separate and independent of Avaya IP Softphone licenses, which are required for Avaya IP Softphones but not required for AES DMCC stations. Enter the **display system-parameters customer-options** command and verify that there are sufficient IP\_API\_A licenses. If not, contact an authorized Avaya account representative to obtain these licenses.

```

display system-parameters customer-options                    Page 10 of 11
                                MAXIMUM IP REGISTRATIONS BY PRODUCT ID

Product ID  Rel. Limit  Used
IP_API_A   : 200       0
IP_API_B   : 0         0
IP_API_C   : 0         0
IP_Agent   : 50        0
IP_IR_A    : 0         0
IP_Phone   : 12000     3
IP_ROMax   : 12000     0
IP_Soft    : 2         0
IP_eCons   : 0         0
           : 0         0
           : 0         0

```

Enter the **add station s** command, where **s** is an extension valid in the provisioned dial plan. On **Page 1** of the STATION form, set the Type field to an IP telephone set type, enter a descriptive Name, specify the Security Code, and set the IP SoftPhone field to **y**. During the compliance test, the set type 4620 was used for recording stations.

Repeat this as necessary, with the same Security Code, to configure additional DMCC stations. For the compliance test, stations from 23001 to 23046 were created for the purpose of recording. When multiple stations are involved, consider using the **duplicate station** command.

add station 23001		Page 1 of 4
STATION		
Extension: 23001	Lock Messages? n	BCC: 0
Type: 4620	Security Code: *	TN: 1
Port: ip	Coverage Path 1:	COR: 1
Name: DMCC -1	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 23001	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Expansion Module? n	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	

### 3.5. Recorded Stations

Enter the **add station s** command, where **s** is an extension valid in the provisioned dial plan. On **Page 1** of the STATION form, set the Type field to an IP telephone set type, enter a descriptive Name, and specify the Security Code. For the compliance test, recorded stations from 22001 to 22009 were created.

add station 22001		Page 1 of 4
STATION		
Extension: 22001	Lock Messages? n	BCC: 0
Type: 4621	Security Code: *	TN: 1
Port: S00142	Coverage Path 1:	COR: 1
Name: 72001	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 22001	
Display Language: english	Mute Button Enabled? y	
Survivable GK Node Name:	Expansion Module? n	
Survivable COR: internal		
Survivable Trunk Dest? y	Media Complex Ext:	
	IP SoftPhone? n	
	Customizable Labels? y	

On **Page 3** of the STATION form, for ABBREVIATED DIALING List 2, enter the abbreviated dialing group configured in **Section 3.3**. Configure the following BUTTON ASSIGNMENTS in addition to the call-appr (call appearance) buttons:

- auto-in
- aux-work
- abrv-dial – for Login
- abrv-dial – for Logout.

add station 22001		Page 3 of 4	
STATION			
SITE DATA			
Room:		Headset?	n
Jack:		Speaker?	n
Cable:		Mounting:	d
Floor:		Cord Length:	0
Building:		Set Color:	
ABBREVIATED DIALING			
List1: personal 1	List2: group 1	List3:	
BUTTON ASSIGNMENTS			
1: call-appr	5: auto-in	Grp:	
2: call-appr	6: aux-work	RC: Grp:	
3: call-appr	7: abrv-dial	List: 2 DC: 11	
4:	8: abrv-dial	List: 2 DC: 12	

## 4. Configure Avaya Application Enablement Services

The Avaya Application Enablement Services (AES) server enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Avaya Communication Manager. The Avaya Application Enablement Services (AES) server receives requests from CTI applications, and forwards them to Avaya Communication Manager. Conversely, the Avaya Application Enablement Services (AES) server receives responses and events from Avaya Communication Manager and forwards them to the appropriate CTI applications.

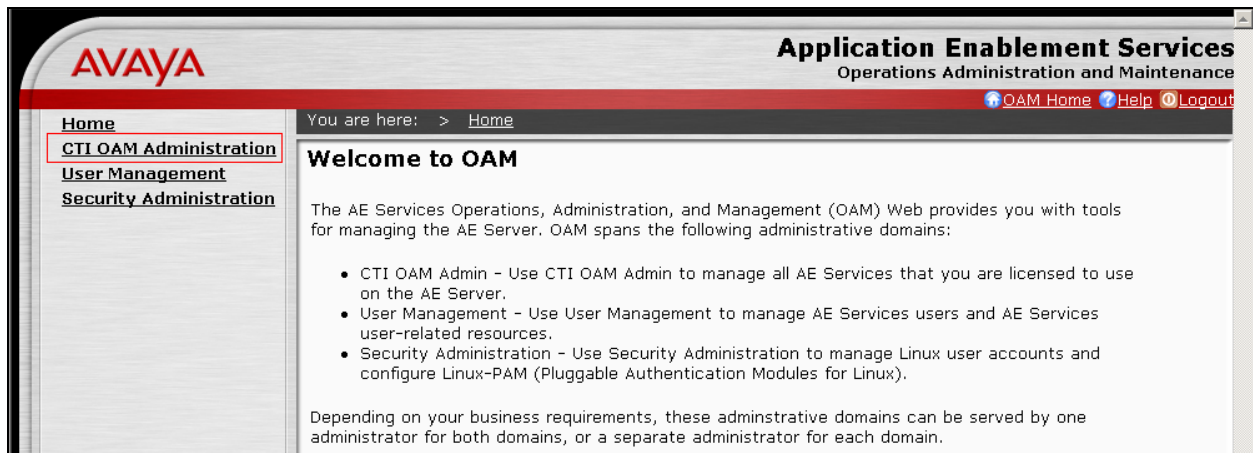
This section assumes that installation and basic administration of the Avaya Application Enablement Services server has been performed. The steps in this section describe the configuration of a Switch Connection, a CTI user, a CMAPI port, and creating a CTI link for TSAPI.

### 4.1. Configure Switch Connection

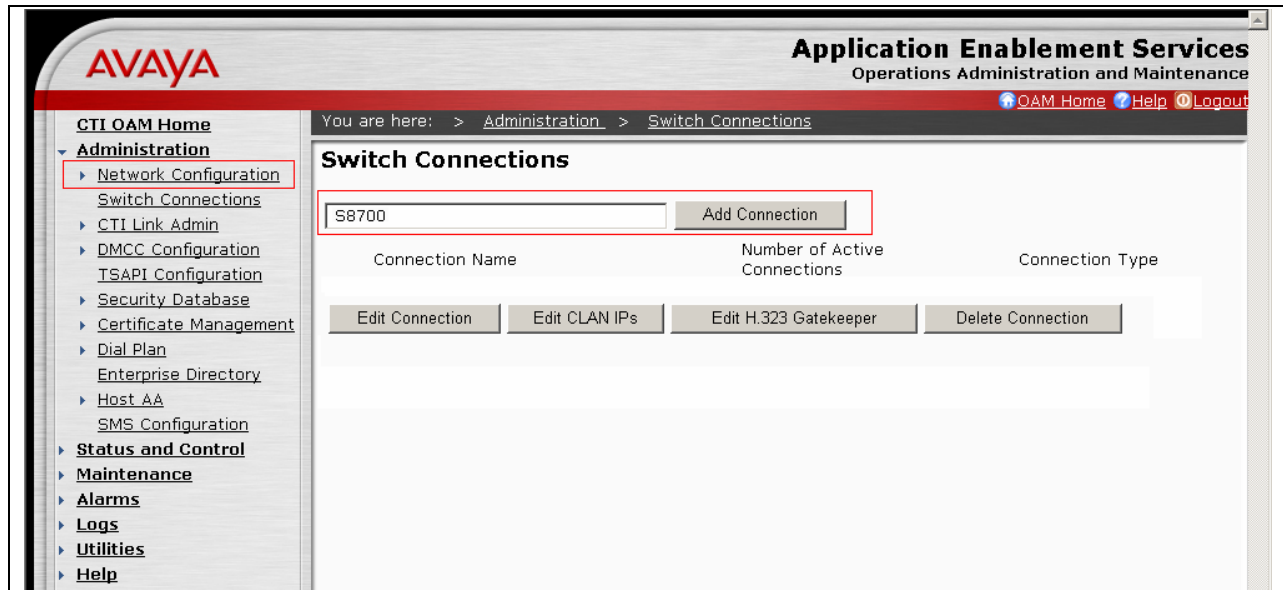
Launch a web browser, enter <https://<IP address of AES server>:8443/MVAP> in the address field, and log in with the appropriate credentials for accessing the AES CTI OAM pages.



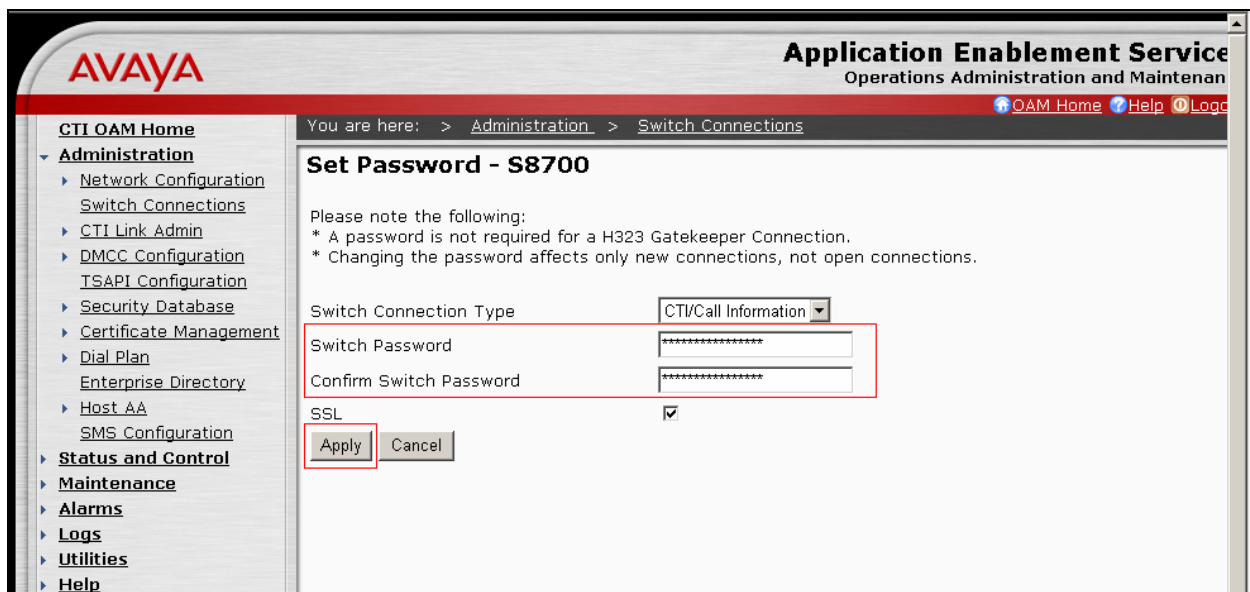
Select the **CTI OAM Administration** link from the left pane of the screen.



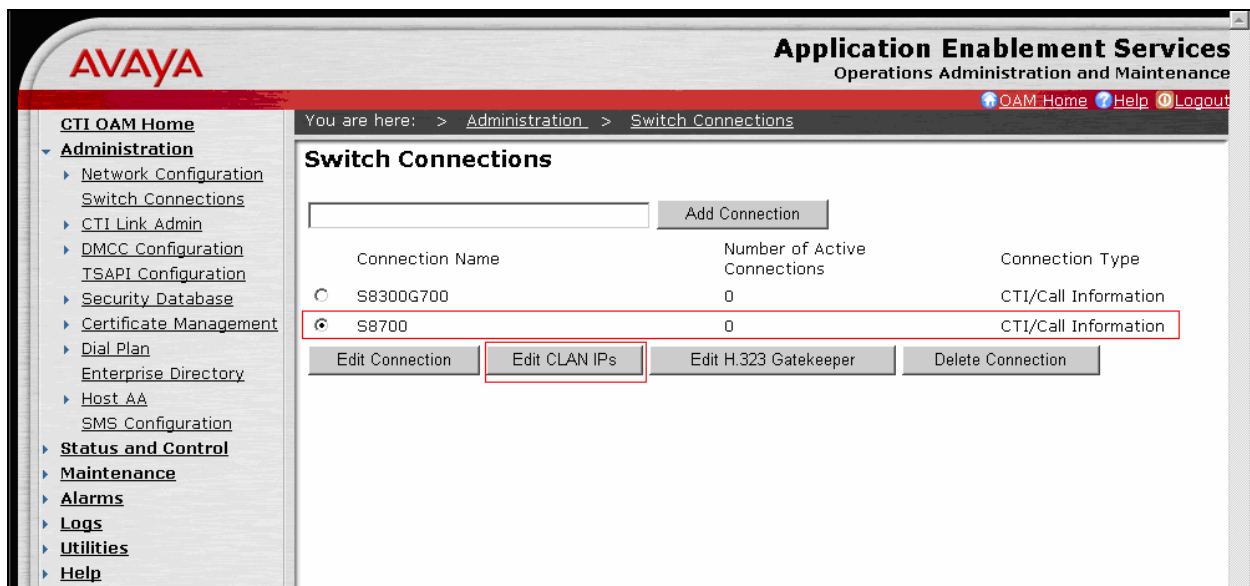
Click on **Administration** → **Switch Connections** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the Avaya AES and Avaya Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.



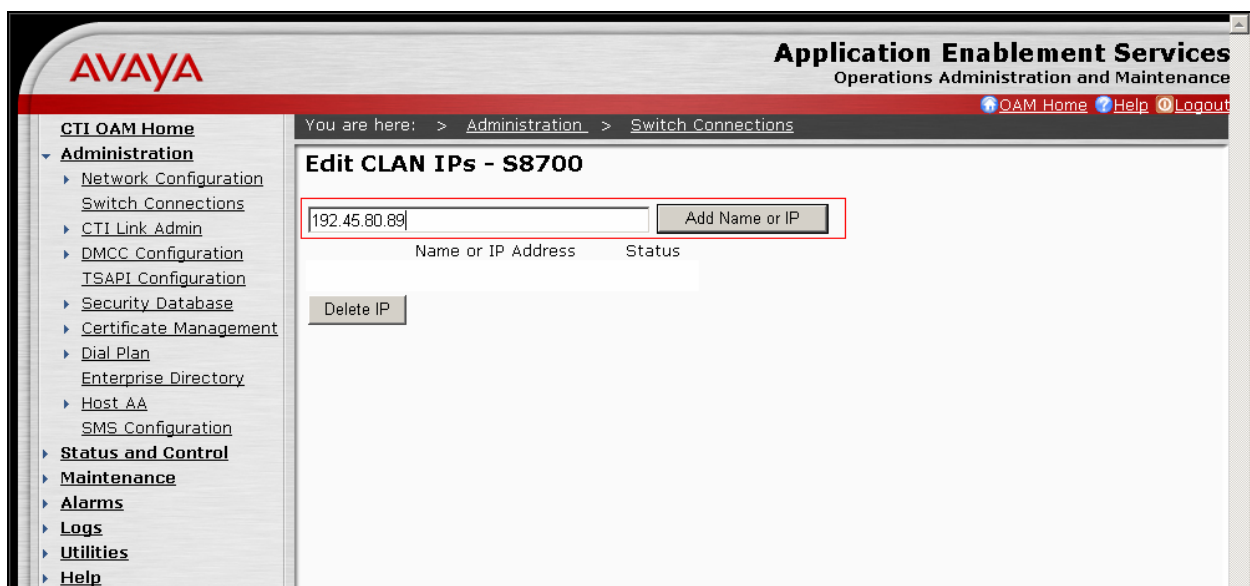
The next window that appears prompts for the Switch Connection password. Enter the same password that was administered in Avaya Communication Manager in **Section 3.1**. Default values may be used in the remaining fields. Click on **Apply**.



After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on **Edit CLAN IPs**.



Enter the CLAN-AES IP address which was configured for AES connectivity in **Section 3.1** and click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.



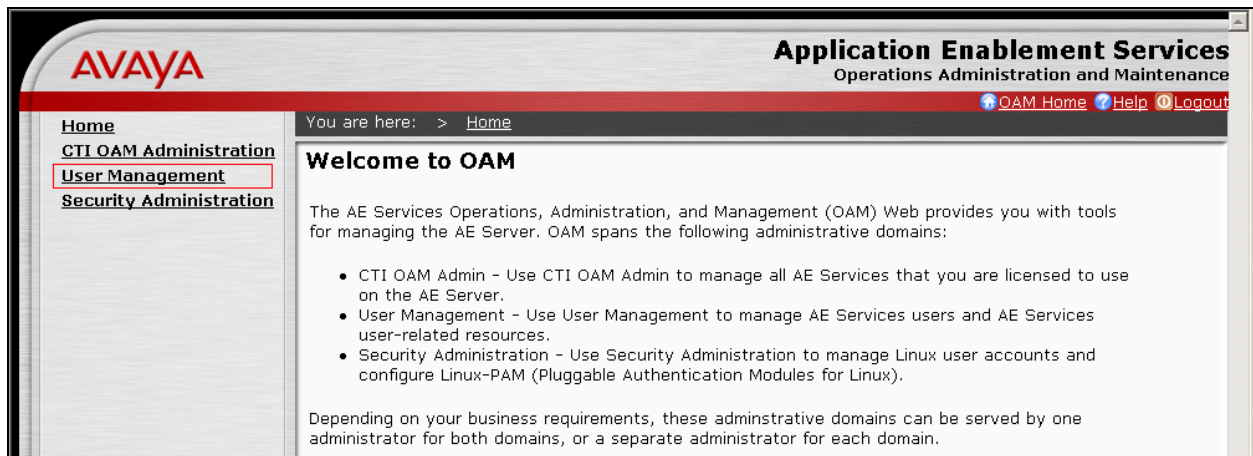
## 4.2. Configure the CTI Users

The steps in this section describe the configuration of a CTI user. Launch a web browser, enter <https://<IP address of AES server>:8443/MVAP> in the URL, and log in with the appropriate credentials to access the relevant administration pages.

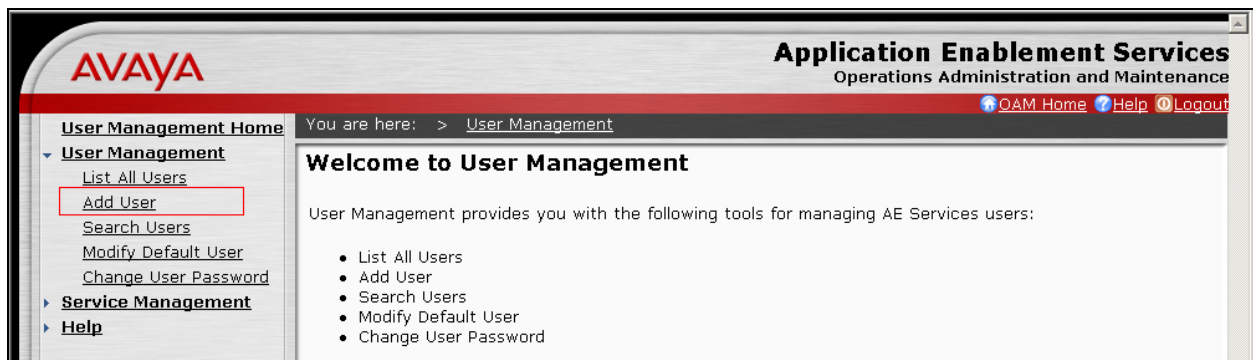




The Welcome to OAM page is displayed next. Select **User Management** from the left pane.



From the Welcome to User Management page, navigate to the **User Management** → **Add User** page to add a CTI user.



On the Add User page, provide the following information:

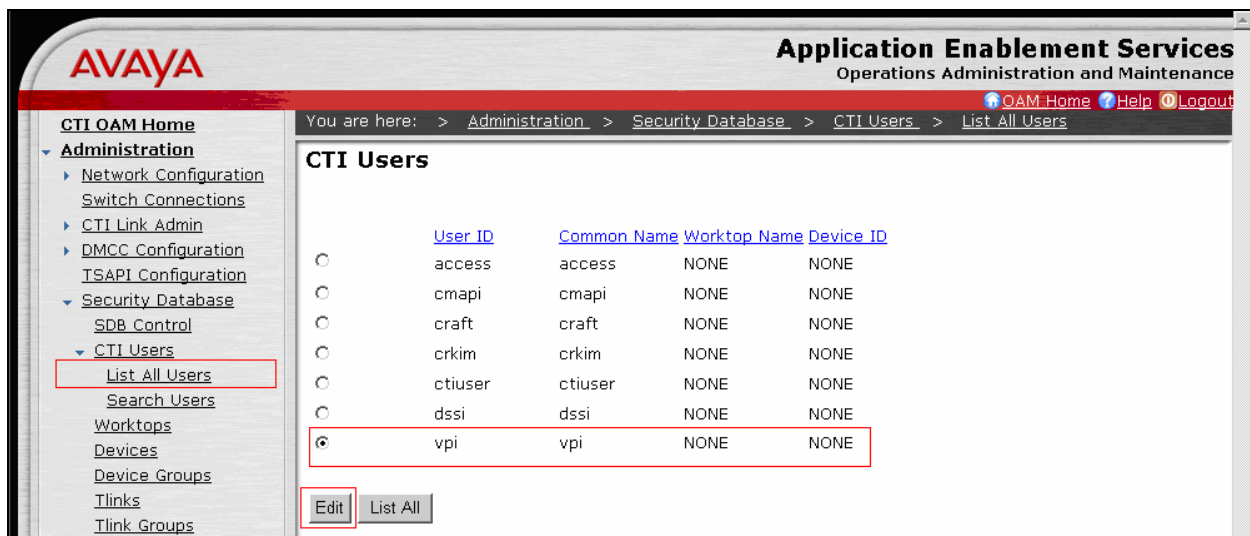


- User Id
- Common Name
- Surname
- User Password
- Confirm Password

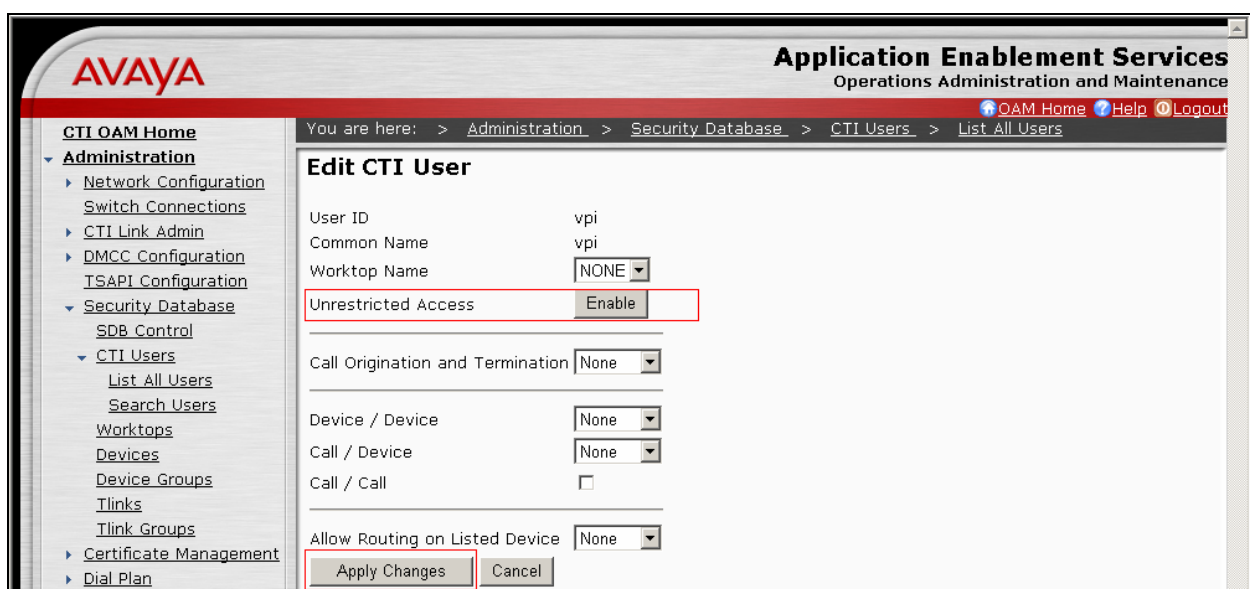
The above information (User ID and User Password) must match with the information configured in the Voice Print Server Configuration page in **Section 5**.

Select **Yes** using the drop down menu on the CT User field. This enables the user as a CTI user. Click the **Apply** button (not shown) at the bottom of the screen to complete the process. Default values may be used in the remaining fields.

Once the user is created, select **OAM Home** in upper right and navigate to the **CTI OAM Administration → Security Database → CTI Users → List All Users** page. Select the User ID created previously, and click the **Edit** button to set the permission of the user.



Provide the user with unrestricted access privileges by clicking the **Enable** button on the Unrestricted Access field. Click the **Apply Changes** button.



Navigate to the **CTI OAM Home** → **Administration** → **Ports** page to set the DMCC server port. During the compliance test, the default port values were utilized. The following screen displays the default port values. Since the unencrypted port was utilized during the compliance test, set the Unencrypted Port field to **Enabled**. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process. Default values may be used in the remaining fields.

AVAYA

Application Enablement Services

Operations Administration and Maintenance

[OAM Home](#)
[Help](#)
[Logout](#)

CTI OAM Home

Administration

Network Configuration

Local IP

NIC Configuration

Ports

Switch Connections

CTI Link Admin

DMCC Configuration

TSAPI Configuration

Security Database

Certificate Management

Dial Plan

Enterprise Directory

Host AA

SMS Configuration

Status and Control

Maintenance

Alarms

Logs

Utilities

Help

You are here: > Administration > Network Configuration > Ports

Ports

CVLAN Ports

Unencrypted TCP Port

9999

Enabled Disabled

Encrypted TCP Port

9998

Enabled Disabled

DLG Port

TCP Port

5678

TSAPI Ports

TSAPI Service Port

450

Enabled Disabled

Local TLINK Ports

TCP Port Min

1024

TCP Port Max

1039

Unencrypted TLINK Ports

TCP Port Min

1050

TCP Port Max

1065

Encrypted TLINK Ports

TCP Port Min

1066

TCP Port Max

1081

DMCC Server Ports

Unencrypted Port

4721

Enabled Disabled

Encrypted Port

4722

Enabled Disabled

TR/87 Port

4723

Enabled Disabled

H.323 Ports

TCP Port Min

3000

TCP Port Max

4100

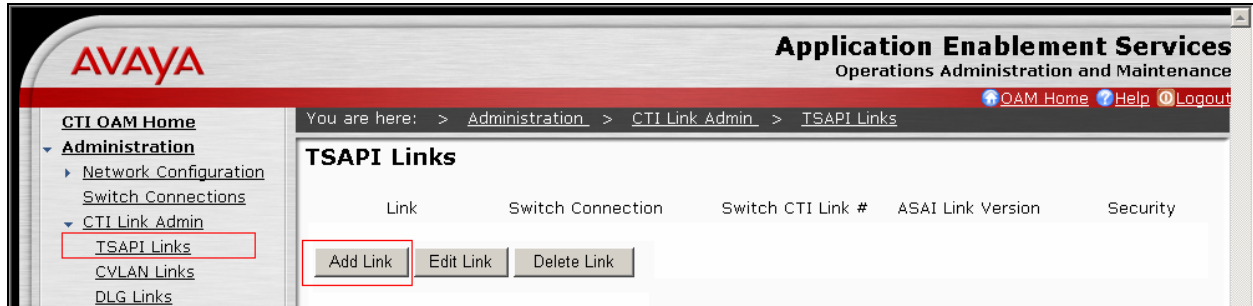
CRK; Reviewed:  
SPOC 4/15/2008

Solution & Interoperability Test Lab Application Notes  
©2008 Avaya Inc. All Rights Reserved.

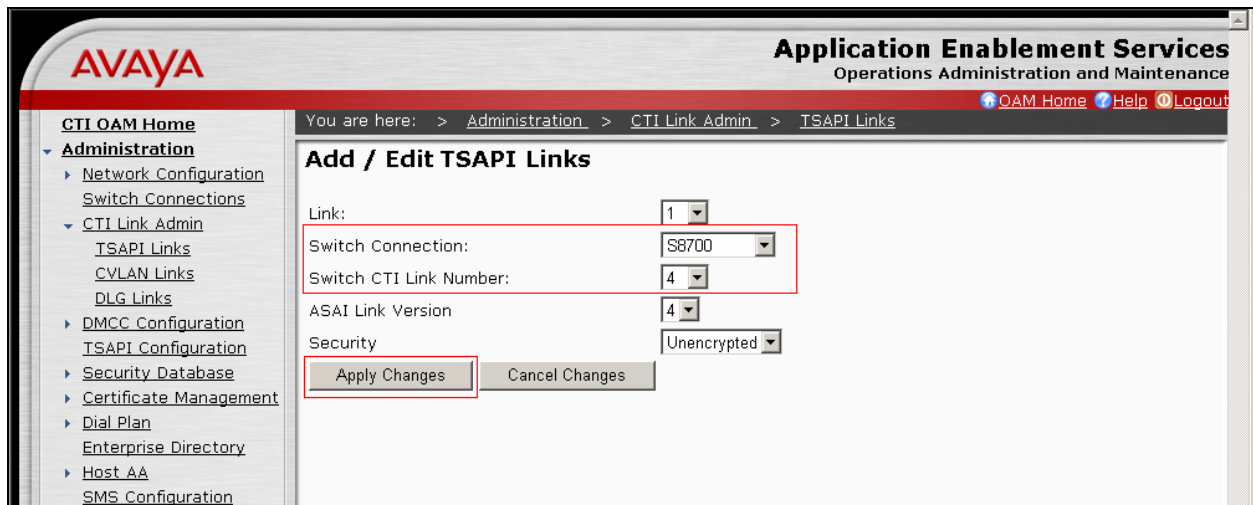
19 of 24  
VPI-ACM-AES41

### 4.3. Configure the TSAPI CTI Link

Navigate to the **OAM Home** → **CTI OAM Admin** → **Administration** → **CTI Link Admin** → **TSAPI Links** page to set the TSAPI CTI Link. Click on **Add Link**.



Select a Switch Connection using the drop down menu. The Switch Connection is configured in **Section 4.1**. Select the Switch CTI Link Number using the drop down menu. Switch CTI Link Number should match with the number configured in the cti-link form in **Section 3.1**. Click the **Apply Changes** button. Default values may be used in the remaining fields.



## 5. Configure the Voice Print Activ! Voice Call Logger

Voice Print installs, configures, and customizes the Activ! Voice Call Logger application for their end customers. This section only describes the interface configuration for the Activ! Voice Call Logger application to communicate with Avaya AES and Avaya Communication Manager. Refer to [3] for configuring the Voice Print Activ! Voice Call Logger application.

The following screen shows the Voice Print Server Configuration page. Provide the following information:

- **Server Machine Name** – Provide a Tlink name. To get the Tlink name, navigate to the **Administration** → **Security Database** → **Tlinks** page from the CTI OAM Home page in Avaya AES.

- Application User Name – Provide a User Id, created in **Section 4.2**.
- Application Password – Provide a User Password, created in **Section 4.2**.
- Server IP Address – Provide Avaya AES Client Connectivity IP address. The IP address can be obtained by navigating to the **Administration → Network Configuration → Local IP** page from the CTI OAM Home page in Avaya AES.
- Server Port – During the compliance test, the unencrypted port, 4721, was utilized.
- Switch (CLAN) Address – The CLAN IP address, which was utilized for registering AES DMCC stations.

Click on Apply to submit the changes.

The screenshot shows the 'Voice Print Server Configuration' window with the 'TSAPI' tab selected. The left sidebar shows a tree view with 'Server localhost' expanded, and 'Channel Manager' selected. The main area contains several configuration sections:

- TSAPI Server Setup:**
  - Server Machine Name: AVAYA#S8700#CSTA#
  - TSAPI Device Name: (empty)
  - Application User Name: vpi
  - Application Password: vpi
  - ☐ Fail to VDX
  - ☐ Save All ANI
- General Options:**
  - ☒ Record All Agents
  - ☐ Lock Status Lights
  - ☐ Use TSAPI Time Stamp
- Additional Monitors:**
  - ACD Groups: 50011
  - Trunks: (empty)
- Service Observe Options:**
  - ☒ Monitor Agent Mode Change
  - Feature Code: (empty)
- Switch Type:**
  - ☒ CSTA Compliant
  - ☐ Avaya / Lucent
  - ☐ Nortel Meridian
  - ☐ Aspect
  - ☐ NEC
- CMAPI (AES) Options:**
  - ☒ Enable
  - First Extension: 23001
  - Extension Password: (empty)
  - Server IP Address: 192.45.85.102
  - Server Port: 4721
  - Switch (CLAN) Address: 192.45.80.87

At the bottom right, there are 'Apply' and 'Cancel' buttons. The status bar at the bottom shows 'Offline' and 'AGENT: 1'.

## 6. Interoperability Compliance Testing

The interoperability compliance test included feature, serviceability, and performance testing. The feature testing evaluated the ability of the Voice Print Activ! Voice Call Logger to monitor and record calls placed to and from stations and to VDNs. The serviceability testing introduced failure scenarios to see if the Voice Print Activ! Voice Call Logger can resume recording after failure recovery. The performance testing stressed the Voice Print Activ! Voice Call Logger by continuously placing calls over extended periods of time.

## 6.1. General Test Approach

The general approach was to place various types of calls to and from stations, agents, and VDNs, monitor and record them using the Voice Print Activ! Voice Call Logger, and verify the recordings. For feature testing, the types of calls included internal calls, inbound and outbound trunk calls, transferred calls, bridged calls, and conferenced calls. Performance tests verified that the Voice Print Activ! Voice Call Logger could record calls during a sustained, high volume of calls. For serviceability testing, failures such as cable pulls, CTI link busyouts and releases, and resets were applied.

## 6.2. Test Results

All test cases were executed and passed.

## 7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Communication Manager and Avaya AES.

### 7.1. Verify Avaya Communication Manager

Verify the status of the administered AES link by using the **status aesvcs link** command.

```
status aesvcs link
```

AE SERVICES LINK STATUS						
Srvr/ Link	AE Services Server	Remote IP	Remote Port	Local Node	Msgs Sent	Msgs Rcvd
01/01	server1	192. 45. 80.102	36538	CLAN-AES	17	18

Verify the status of the administered TSAPI CTI link by using the **status aesvcs cti-link** command.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
2		no	server1	restarting	15	15
4	4	no	server1	established	15	15

### 7.2. Verify Avaya Application Enablement Services

From the CTI OAM Admin web pages, verify the status of the TSAPI and DMCC Services are ONLINE, by selecting **Status and Control → Services Summary** from the left pane.

Service	Status	Since	Cause
CVLAN Service	ONLINE	2007-12-12 20:47:41	NORMAL
DLG Service	ONLINE	2007-12-12 20:47:36	NORMAL
TSAPI Service	ONLINE	2007-12-12 20:47:43	NORMAL
DMCC Service	ONLINE	2007-12-12 20:47:44	NORMAL

## 8. Support

Technical support for the Voice Print Activ! Voice Call Logger can be obtained by contacting VPI via the support link at <http://support@vpi-corp.com> or by calling the support telephone number at 1-805-389-5201.

## 9. Conclusion

These Application Notes illustrate the procedures for configuring the Voice Print Activ! Voice Call Logger call recording solution to monitor and record calls placed to and from stations and to VDNs on an Avaya Communication Manager system. In the configuration described in these Application Notes, the Voice Print Activ! Voice Call Logger employs Device, Media and Call Control Application Programming Interface virtual stations as recording ports. During compliance testing, the Voice Print Activ! Voice Call Logger successfully monitored events and recorded calls placed to and from stations, as well as calls placed to VDNs and then queued to an agent hunt/skill group. The Voice Print Activ! Voice Call Logger was also able to record calls under continuous call volumes over extended periods of time.

## 10. Additional References

This section references the Avaya and Voice Print documentation that are relevant to these Application Notes.

The following Avaya product documentation can be found at <http://support.avaya.com>.

[1] *Feature Description and Implementation for Avaya Communication Manager*, Issue 5, February 2007, Document Number 555-245-205.

[2] *Application Enablement Services Administration and Maintenance Guide*, Release 4.1, Issue 8, December 2007, Document Number 02-300357

The following documentation was provided by Voice Print

[3] *VPI ACTIV! VOICE TSAPI CHANNEL MANAGER APPLICATION NOTES*, May 11 2007.



---

**©2008 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).